IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA

v.

ZACHARY LEE SHAMES,
Defendant

Criminal No. 1:16-cr-289

STATEMENT OF FACTS

The United States and the defendant, ZACHARY LEE SHAMES, agree that the following facts are true and correct, and that had this matter proceeded to trial, the United States would have proven them beyond a reasonable doubt with admissible and credible evidence that from on or about January 2012 through on or about March 17, 2015, the defendant aided and abetted the commission of computer intrusions, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 2. Specifically, at all relevant times, the defendant committed the acts specified below knowing that some of his customers intended to use the keylogger he designed to knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization to 10 or more protected computers during any one year period, and with the purpose of aiding the commission of those crimes, and causing them to be committed.

The United States and the defendant further agree that the following facts are true and would have been established at trial beyond a reasonable doubt through credible and admissible evidence:

1. The defendant, ZACHARY LEE SHAMES is currently enrolled at James Madison University (JMU) and is majoring in computer science. SHAMES was born on August

18, 1995, and enrolled at JMU in the fall of 2013. SHAMES ran the illegal business described in this statement of facts both from his dorm room at JMU, and previously from his parents' house in Great Falls, Virginia, while in high school within the Eastern District of Virginia.

2. Between on or about January 2012 through on or about December 2014, SHAMES developed, marketed, and sold computer keylogger software (hereinafter, the "Keylogger"). One purpose of the Keylogger was to access without authorization sensitive information, such as passwords, on the computers on which the software was installed and send the stolen data to a website or email account designated by its users.

3. The Keylogger offered various features, including, but not limited to, the following:

a. the ability to recover all keystrokes typed on the victim's computer or only custom keystrokes, such as those entered into a web browser;

b. the ability to recover the victim's passwords stored in a web browser or other program;

c. the ability to resume keylogging every time the victim's computer restarts;

d. the ability to clear web browser cookies, which would force the victim to retype her online usernames and passwords;

e. the ability to send screenshots of the victim's computer;

f. the ability to spread the keylogging software to the victim's "friends" or "buddies" on certain services through a custom message sent from the victim's account; and

g. the ability to scan the keylogger against dozens of anti-virus services to determine whether the keylogger will be flagged by those services.

4. SHAMES sold the Keylogger to at least 3,112 users who, in turn, used the Keylogger to infect at least 16,847 computers. SHAMES typically sold the Keylogger for $15-$40, and in one instance customized the Keylogger to the customer's specifications for $150.00. SHAMES advertised the Keylogger on webforums devoted to computer hacking and accepted payment through PayPal and Bitcoin. SHAMES received at least $60,993 in payments for the Keylogger to his PayPal account alone. SHAMES paid others from these proceeds for assistance in developing the Keylogger and related materials, as well as for assistance in selling the Keylogger.

5. SHAMES designed the Keylogger for the purpose of allowing users to access victim computers without authorization and steal information of value, such as passwords and other personal information, from the victim computers. At all relevant times, SHAMES understood that his software was being used for such purposes, and knew that his customers could use the stolen information to spy on the victims and/or to commit fraud.

6. After releasing the initial version of the Keylogger, SHAMES and others created several updated versions of the Keylogger in response to the concerns of his customers, including concerns about whether the Keylogger would be detected by the anti-virus systems of the victims' computers.

7. SHAMES helped further the criminal aims of his customers after sale by providing customer support via email, Skype, and discussions on websites devoted to computer hacking.

8. For instance, during a Skype conversation on or about December 14, 2014, a customer told SHAMES the following:

> i used your … keylogger
> i must commend you

> cos that was a very good keylogger
> PP [Predator Pain] is good but [your keylogger] is still the best
> i have PP but i have more trust in you
> and beleive your custom kL will beat any thing else
> I want you to build be a keylogger with the best password revovery tool
> having the ability to recover passwords from all latest browsers,
> messengers, ftps, putty and pop accounts
> and also all filled forms
> i also want the keylogger to be able to be backdoored
> meaning i can put the download link to my rat server while
> building a keylogger bin
> so that once victim clicks the keylogger bin
> both the keylogger and rat [Remote Administrative Tool] will run
> on the victims computer
> so i will keylogger and rat the system by just spreading one file
> predator pain has this option but its not functioning
> i want it to keylog and cliboard log as well as screen short capturing
> and as you said...should be FUD
> thats all for now

SHAMES responded: "I should be able to do it, although, the stealers will make the project more expensive." After negotiating with the customer, SHAMES offered the following:

> that would be $150
> well, stealers are slightly different
> its $130 if you count the stealers as normal features, but updated
> stealers are hard to come by and I need to recode them. So, as I
> said, they will be slightly more expensive

On or about December 15, 2014, SHAMES provided the customer with the following updates:

> Status Update #1: - Finished Keylogger Base - Finished Chrome,
> IE, and Firefox Stealers
>
> Status Update #2: - Finished Mail Stealers (Needs Testing though)
>
> Status Update #3: - 1/37 so far - Finished startup - Finished
> Downloader - (Finished Entire Stub/Payload)

On or about December 16, 2014, SHAMES provided the customer with the following update:

> Status Update #4: - Did some testing, the stealers work, and the cc
> option for mailing works as well - Logs seem to work as well
> (including IP address)

9. During a Skype conversation on or about December 30 and 31, 2014, SHAMES told a potential customer the following:

> I only make custom keyloggers for people now
> Well the base of the keylogger is $100
> That is the keylogger, and startup
> Other features will cost different depending on the feature
> It is so expensive because it will be FUD [fully undetectable]
> and only used by you
> I only take bitcoin and paypal.

SHAMES asked the customer which features he wanted for the keylogger, and the customer responded as follows:

> monitors and records all activities performed on a computer and
> sends reports to a specified email
> including advanced logviewer, keystroke logging, screenshots
> logging, files logging, printer logging
> * * *
> the most important is to record all keystrocks and recover all
> passwords

SHAMES responded: "I can do this." SHAMES provided the following prices:

> Ok Pricing: - Keylogger: $100 - Email Sending: $0 - FTP Sending:
> $3 - Screenshot logging: $5 - Browser Recovery: $50 -
> Startup/Autorun: $0
> Total: $158

10. On April 23, 2013, SHAMES had a discussion with a customer who complained that "the victim's keyboard after infected will no longer work properly. Victim will call the pc doctor and the logger will be compromised." During the course of his conversation with this customer, SHAMES assured him: "Trust me. I made this logger. I coded it. It doesn't change the way the words are typed."

11. SHAMES also had several discussions with customers on an website devoted to computer hacking in which he instructed them on how his Keylogger could be used to steal email and social media passwords from the victim computers. For instance:

a) On September 27, 2013, a customer posted: "Confirm … Outlook recovery WORKING!," referring to the Keylogger's ability to recover the victims' passwords to Microsoft's popular email service. SHAMES responded, "Thanks for testing and posting this. I hope you enjoy the new update!"

b) On November 2, 2013, a customer asked SHAMES whether the Keylogger "steal[s] saved passwords of [sic] 2014 outlook." SHAMES responded: "Yes it should do that. It has the latest recoveries."

c) On November 4, 2013, a customer asked SHAMES: "still waiting to know if it steals 2014 Outlook." SHAMES responded: "We are 100% sure it recovers 2013 passwords. If anyone wants to test 2014, feel free."

d) On November 21, 2013, a customer asked whether SHAMES whether "this is a worm which grabs the login data, log into a facebook/twitter account and spreads a text." SHAMES replied: "yes, it spreads as many posts as you want, and custom ones too!"

12. In addition, SHAMES produced a Youtube video in which he instructed his customers on how to use the Keylogger. During this video, SHAMES repeatedly uses the term "victims" to refer to the people on whose computers his customers would install the Keylogger.

13. The statement of facts includes those facts necessary to support the defendant's guilty plea. It does not include each and every fact known to the defendant or to the government and it is not intended to be a full enumeration of all of the facts surrounding the defendant's case.

14. The actions of the defendant, as recounted above, were in all respects knowing, voluntary, and intentional, and were not committed by mistake, accident or other innocent reason.

Dana J. Boente
United States Attorney

Date: January ___, 2017

By: _____
Kellen S. Dwyer
Assistant United States Attorney

Ryan K. Dickey, Senior Counsel
U.S. Department of Justice, Criminal Division
Computer Crime & Intellectual Property Section

Defendant's Signature: After consulting with my attorney, I hereby stipulate that the above Statement of Facts is true and accurate and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

Date: 1/12, 2017

Zachary Lee Shames
Defendant

Defense Counsel Signature: I am Zachary Lee Shames's attorney. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

Date: 1/12, 2017

Thomas C. Hill, Esq.
Counsel for the Defendant